IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF WEST VIRGINIA

IN THE MATTER OF THE SEARCH OF ONE BLACK SAMSUNG GALAXY A02 WITH AN IMEI OF 354762611897080 SEIZED FROM 303 ROTHWELL AVE, MARTINSBURG, WEST VIRGINIA AND CURRENTLY LOCATED AT FBI MARTINSBURG FIELD OFFICE	Case No. **3:23mj83**

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Mark McNeal, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and I have been so employed since May 2015. I am currently assigned to Martinsburg, West Virginia Resident Agency of the Pittsburgh Division. I attended the FBI's training academy in Quantico, Virginia, where I received instruction regarding a variety of investigations. I graduated from the FBI training academy as a Special Agent in November 2015. I serve as a member of the Evidence Response Team for the Pittsburg Division. During my time as an FBI Special Agent, I have worked a variety of investigations, including investigations of counterterrorism, domestic terrorism, white-collar crimes, crimes against children and violent

gang offenses. I also have training and experience in obtaining and executing search warrants, interviewing witnesses, and other acts involved in a federal criminal investigation.

3. I make this affidavit in support of an application for a search warrant for an electronic device seized from 303 Rothwell Ave, Martinsburg, West Virginia on March 03, 2023 ("the TARGET DEVICE"), further described in Attachment A.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 922(g)(1) (Prohibited Person in Possession of a Firearm) and 18 U.S.C. § 2261(a)(1) (Interstate Domestic Violence) have been committed by PAUL TOMLINSON (hereafter TOMLINSON), from approximately July 2022 through February 2023. There is also probable cause to believe the TARGET DEVICE contain evidence, instrumentalities, contraband, or fruits of these crimes.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

6. The "TARGET DEVICE" is the following electronic device, which was seized from 303 Rothwell Ave, Martinsburg, West Virginia, on March 3, 2023.

a. Black-in-color Samsung Galaxy A02s with cracked screen and a serial number of R9HR903XCQY and an IMEI of 354762611897080 (further described in Attachment A)

7. The TARGET DEVICE is currently stored in the Evidence Room at the FBI, 1250 Edwin Miller Boulevard, Martinsburg, West Virginia, in the Northern District of

West Virginia. Based on training and experience, your affiant knows the TARGET DEVICE has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the TARGET DEVICE first came into the FBI's possession.

8. The applied-for warrant would authorize the forensic examination of the TARGET DEVICE for the purpose of identifying the electronically stored information particularly described in Attachment B.

DEFINITIONS

9. The following definitions apply to this affidavit and to Attachment B:

a. "Cellular telephone" or "wireless telephone" means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving videos; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geographic information indicating where the cell phone was at particular times.

b. "Computer", as used herein, is defined pursuant to Title 18, United States Code, Section 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

c. "Computer hardware", as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, laptops, tablets, eReaders, Notes, iPads, and iPods; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, SD cards, thumb drives, flash drives, USB storage devices, CDs and DVDs, and other memory storage devices); peripheral input/output devices (including, but not limited to keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

d. "Computer software", as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

e. "Computer-related documentation," as used herein, consists of electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

f. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

g. "Electronic storage devices" includes computers, cellular telephones, tablets, and devices designed specifically to store electronic information (e.g., external hard drives and USB "thumb drives"). Many of these devices also permit users to communicate electronic information through the Internet or through the cellular telephone network (e.g., computers, cellular telephones, and tablet devices such as an iPad).

h. "Tablet," as used herein, is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access

the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

i. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

j. "Internet Service Providers" (ISPs) are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone-based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider (ISP)

over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

k. "An Internet Protocol address" (IP address) is a unique numeric address used by Internet-enabled electronic storage devices to access the Internet. Every electronic storage device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that electronic storage device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static— that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

l. The terms "documents" and "materials" include all information recorded in any form, visual or aural, and by any means, whether in electrical, electronic or magnetic form (including tape recordings, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks (DVDs), Multi Media Cards (MMCs), memory sticks, smart cards, or electronic notebooks, as well as digital data files and or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTERS AND CRIMINAL ACTIVITY

10. Due to your affiant's training and experience, he knows that persons involved in the unlawful purchase of a firearm and crimes of violence, such as that described herein, utilize communication methods, namely wireless telephones, to plan, coordinate and conduct their crimes. Evidence of this activity in the form of call logs, stored Short Message Services (SMS) text messages, emails, Internet history and other data is stored within the

internal memory of the devices used. This evidence is often critical to establishing the criminal conduct of the subjects using the devices.

PROBABLE CAUSE

11. On March 1, 2023, the Martinsburg Police Department (MPD) was called to 303 Rothwell Ave for a domestic altercation in progress. It was initially reported as a fight between Jarrod Bedilion and his stepdaughter's boyfriend, TOMLINSON. Upon further investigation, MPD was informed that TOMLINSON had physically abused the stepdaughter, SJ, his girlfriend who is on the autism spectrum, during a cross-country road trip that lasted more than six months. It was also reported that TOMLINSON owned a firearm that was located inside the vehicle belonging to SJ. TOMLINSON was arrested and a search was conducted of the vehicle belonging to SJ, which TOMLINSON and SJ drove during their cross-country trip. Items found inside the vehicle included a Ruger SR-22 (.22 caliber pistol), .22 caliber ammunition, TOMLINSON's driver's license and his cellular telephone (TARGET DEVICE). MPD seized the firearm, ammunition, and driver's license.

12. The TARGET DEVICE was left with the car located at 303 Rothwell Ave. During an interview with SJ, the FBI identified that the TARGET DEVICE belonged to TOMLINSON and had been in his possession during the entirety of their cross-country road trip. The TARGET DEVICE was seized from SJ's vehicle at 303 Rothwell Avenue and held in the Martinsburg FBI Evidence Room.

13. On March 2, 2023, your affiant interviewed SJ about her road trip with TOMLINSON. It was decided that SJ should be given a forensic interview due to her status with autism and young age (19 years old). A forensic interview was scheduled and conducted by Safe Haven CAC (now Victoria's House). In that interview, SJ shared specific occurrences

of physical and sexual abuse during their cross-country road trip. There were multiple instances of sexual assault, with each occurring in different states. SJ stated that the two most egregious sexual assaults took place at TOMLISON's father's home in Kentucky (KY) and his mother's home in Delaware (DE). Both instances involved violence, losing consciousness, and at least one occurrence of forcible anal sodomy in Delaware. SJ was clear that physical abuse was a continual occurrence during the entirety of the trip. She noted that she sent photographs to her mother, under TOMLINSON'S supervision and direction, where he would make her smile and appear to be enjoying herself but also where she would subtly show the bruises from the physical abuse. Those digital photographs were shared with the FBI and do appear to show bruising on SJ.

14. During this investigation, your affiant reviewed jail calls made by TOMLINSON, from the Eastern Regional Jail in Martinsburg, WV. On March 4, 2023, TOMLISNON called Family Member 1. In that call, TOMLINSON stated that he did not deserve SJ. He stated that it was eating him up thinking about everything he did to SJ. TOMLINSON stated that SJ did not deserve anything like that. On March 5, 2023, TOMLINSON called Family Member 1. In that call, TOMLINSON stated that when he was with SJ, he was an awful, cruel, mean person.

15. In a jail call made on March 1, 2023, TOMLINSON called Family Member 1. In that call, TOMLINSON stated that he would be in jail for a while unless Family Member 1 could get him a lawyer and make the gun charges disappear. TOMLINSON stated, "Which, all the gun charges disappear if…um." Family Member 1 then stated, "If she claims it was her gun."

16. During the CAC Interview of SJ, she stated that TOMLINSON acquired a firearm in KY during their cross-country road trip. She stated that a childhood friend of TOMLINSON's, named Blake, had sold him the firearm. ATF Special Agent Sabrina Hager interviewed Christopher Blake Hubert III at his home in Lawrenceburg, KY, and determined that he provided the Ruger firearm to the Defendant in exchange for work performed on his farm.

17. TOMLINSON had previously been convicted of a crime punishable by imprisonment for a term exceeding one year under state law, that is, two (2) counts of Complicity to Robbery in the Second Degree, in Anderson County (Ky.) Circuit Court Case No. 16-CR-00078, meaning his knowing possession of a firearm in and affecting interstate commerce is in violation of Title 18, United States Code, Sections 922(g)(1) and 924(a)(8).

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

18. Based on my training, experience, and research, I know the TARGET DEVICE, as an electronic device, has capabilities that allows it to serve as a wireless telephone, computer, tablet, and electronic storage device simultaneously.

19. Based on my knowledge, training, and experience, I know electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the devices. This information can often be recovered with forensic tools.

20. There is probable cause to believe that things that were once stored on the TARGET DEVICE may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered

months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this

evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

21. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the TARGET DEVICE was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the TARGET DEVICE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record

information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the devices. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary

to establish that a particular thing is not present on a storage medium.

22. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the TARGET DEVICE consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

23. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

24. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the TARGET DEVICE described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

Mark McNeal, Special Agent
Federal Bureau of Investigation

Affidavit submitted to me by reliable electronic means and attested to me as true and accurate by telephone or other reliable means consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) before me this 1st day of June, 2023.

THE HONORABLE JAMES P. MAZZONE,
UNITED STATES MAGISTRATE JUDGE